Contents

Executive Summary

This project is centered around enhancing the security of virtualized systems using VMware Security Hardening techniques. The primary goal is to align with business requirements by fortifying system resilience, addressing potential vulnerabilities, and ensuring robust security practices.

The project involves multiple critical tasks, including regular software updates, securing remote access configurations, enforcing strong password policies, and implementing comprehensive monitoring to identify and mitigate threats proactively. These measures aim to create a secure and reliable environment, reducing exposure to cyber risks while improving operational efficiency.

The expected outcomes of this project include a significant reduction in system vulnerabilities, strengthened defense mechanisms, and adherence to industry best practices and compliance standards. By applying these strategies, the project not only protects the infrastructure but also builds a strong foundation for sustainable and secure business operations. This initiative highlights the organization's commitment to maintaining high security standards and ensuring the integrity of its virtualized environments.

Project Team

Mohamad Almasri (101167438):

Skilled in system administration and security practices, contributing knowledge of patching, updates, and security configurations. Brings a focus on project organization and teamwork.

Adeshina Samuel (101501091):

Expertise in configuring firewalls and managing network security. Adds value by ensuring secure connections and system hardening techniques.

Rahul Patel (101378458):

Specialized in automation and unattended updates. Enhances project efficiency by implementing streamlined processes.

Aleksandro Kacorri (101516461):

Experienced in auditing and intrusion detection systems. Contributes to the project by improving monitoring and compliance strategies.

Project Details

Project Purpose:

The purpose of this project is to enhance the security of VMware virtual machines (VMs) by identifying and addressing common vulnerabilities, implementing robust hardening measures, and ensuring alignment with industry-recognized security best practices. Virtual machines are essential components of modern IT infrastructures, but their inherent flexibility and connectivity can also make them targets for potential threats.

This project focuses on closing security gaps by applying a series of proactive and defensive strategies. These include securing remote access protocols, enforcing strong authentication and password policies, configuring firewalls, applying timely updates and patches, and using monitoring tools to detect unusual activities. The goal is to minimize exposure to threats, reduce risks of unauthorized access, and build a resilient, hardened environment that safeguards critical assets.

By implementing these measures, the project not only protects the virtualized systems but also ensures compliance with regulatory and organizational standards, enhancing overall operational integrity and reliability. This initiative reflects a commitment to maintaining a secure, efficient, and future-proof IT infrastructure that supports business continuity.

What is Problem Addressed

VMs are vulnerable to cyberattacks if not properly configured. Weak passwords, open SSH access, and unpatched systems are risks that need addressing.

How is the Problem Addressed

Applying updates and patches.

Securing SSH by disabling root login and changing default ports.

Configuring firewalls, enforcing password policies, and monitoring logs.

Required Resources

Hardware: VMware-compatible systems.

Software: Ubuntu Server/Desktop, VMware Workstation.

Tools: Fail2Ban, AppArmor, auditing tools, MFA applications.

Skills

Required Resources

- **Hardware**: VMware-compatible systems.
- **Software**: Ubuntu Server/Desktop, VMware Workstation.
- **Tools**: Fail2Ban, AppArmor, auditing tools, MFA applications.
- **Skills**: Security hardening, system monitoring, vulnerability detection.

Deliverables

This project aims to produce the following comprehensive deliverables:

Secured Virtual Machines (VMs)

Fully configured and hardened Ubuntu Desktop VMs with applied security measures.

Implementation of robust firewall settings, SSH hardening, and strong authentication policies.

Detailed Documentation

- A step-by-step installation and configuration guide for all hardening measures, including screenshots and command references.

  Reports on identified vulnerabilities and the corresponding solutions implemented.

- Automated Update Mechanism

  A fully functional unattended-upgrades system to ensure timely application of critical patches without manual intervention.

- Vulnerability Scan Report

  Results from tools like Nessus, Lynis, or Fail2Ban, showing identified vulnerabilities and proof of resolution.

- Monitoring and Auditing Logs

  Comprehensive system activity logs demonstrating the successful implementation of monitoring tools like auditd and Logwatch.

- AppArmor Configuration

Customized profiles ensuring applications run securely within defined boundaries.

- Multi-Factor Authentication (MFA)

  Integration of MFA for SSH access, showcasing additional layers of security beyond traditional password authentication.

- Team Contributions Summary

  Clear documentation of each team member's role, contributions, and tasks completed throughout the project.

- Compliance with Best Practices

A final review and checklist demonstrating adherence to VMware and Ubuntu security hardening guidelines.

- Technical Presentation

  A formal presentation summarizing the project's objectives, methodology, and results, suitable for technical stakeholders.

Challenges

Technical Challenges

1. ### Challenge: SSH Security Vulnerabilities

   Explanation:

   The default SSH configuration (port 22 and root login enabled) is a common target for brute-force and unauthorized access attempts. This posed a significant risk to system security.

   Work-Around:

   Disabled root login in the SSH configuration file (/etc/ssh/sshd_config).

   Changed the default port to a non-standard port, such as 2222.

   Enabled Fail2Ban to monitor and block repeated unauthorized login attempts.

2. ### Challenge: Configuring a Firewall with UFW

   Explanation:

   Setting up a firewall using UFW (Uncomplicated Firewall) to allow only necessary connections while blocking unauthorized traffic was tricky due to ensuring no essential services were inadvertently blocked.

   Work-Around:

   Carefully reviewed system requirements to identify necessary ports (SSH, HTTP).

   Allowed essential traffic while denying all other connections.

3. **Challenge: Enforcing Strong Password Policies**

Explanation:
By default, there were no strict password requirements, which could allow users to set weak passwords, increasing the risk of unauthorized access.

Work-Around:

Installed and configured libpam-pwquality to enforce minimum password length, complexity, and history.

Educated team members on the importance of strong passwords.

Non-Technical Challenges

1. Challenge: Team Coordination

Explanation:

With team members having different schedules and availability, aligning work sessions and ensuring consistent communication was difficult. This caused delays in task completion and misunderstandings about responsibilities.

Solution:

Established a shared calendar to plan meetings and deadlines.

Used collaboration tools like Microsoft Teams and Google Docs to communicate and work asynchronously.

Conducted weekly check-ins to track progress and address issues.

2. Challenge: Managing Time and Deadlines

Explanation:

Balancing this project with other academic and personal responsibilities made it challenging for some members to meet deadlines. This resulted in last-minute work and increased stress levels.

Solution:

Broke the project into smaller milestones with clear deadlines.

Assigned tasks with realistic timelines based on each member's availability.

Prioritized critical components first to ensure the project remained on

Appendices

Teamwork Allocation

Mohamad Almasri:

Completed all the reports and performed the system installations, ensuring detailed documentation, screenshots, and proper configuration of the system.

Adeshina Samuel:

Took primary responsibility for auditing tasks and verifying system compliance and configurations.

Rahul Patel:

Designed and prepared the PowerPoint presentation, ensuring the project's key findings and results were effectively presented.

Aleksandro Kacorri:

Took primary responsibility for auditing tasks and verifying system compliance and configurations.

References & Citations

VMware Security Hardening Guidelines.

https://www.vmware.com/solutions/security/hardening-guides

Ubuntu Security Documentation.

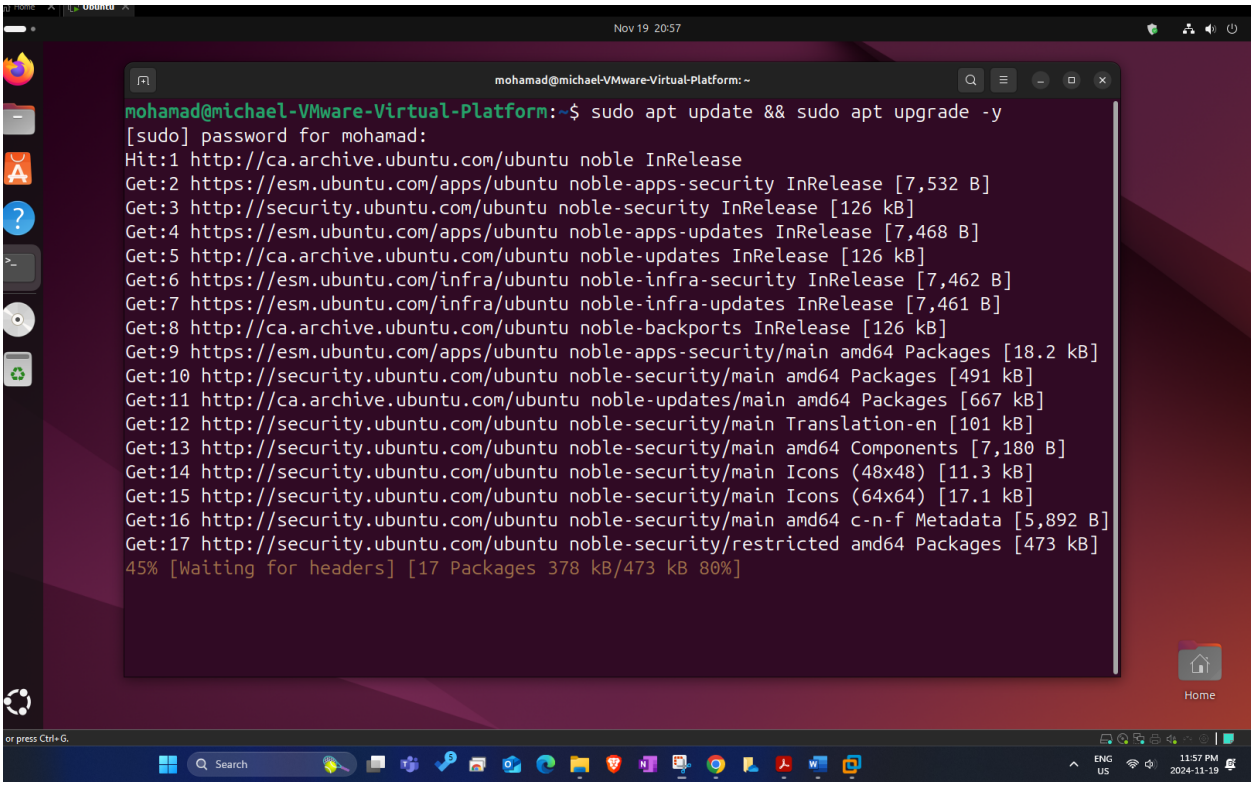
https://ubuntu.com/security/certifications/docs/usg

Installation Documentation

Update and Patch the System

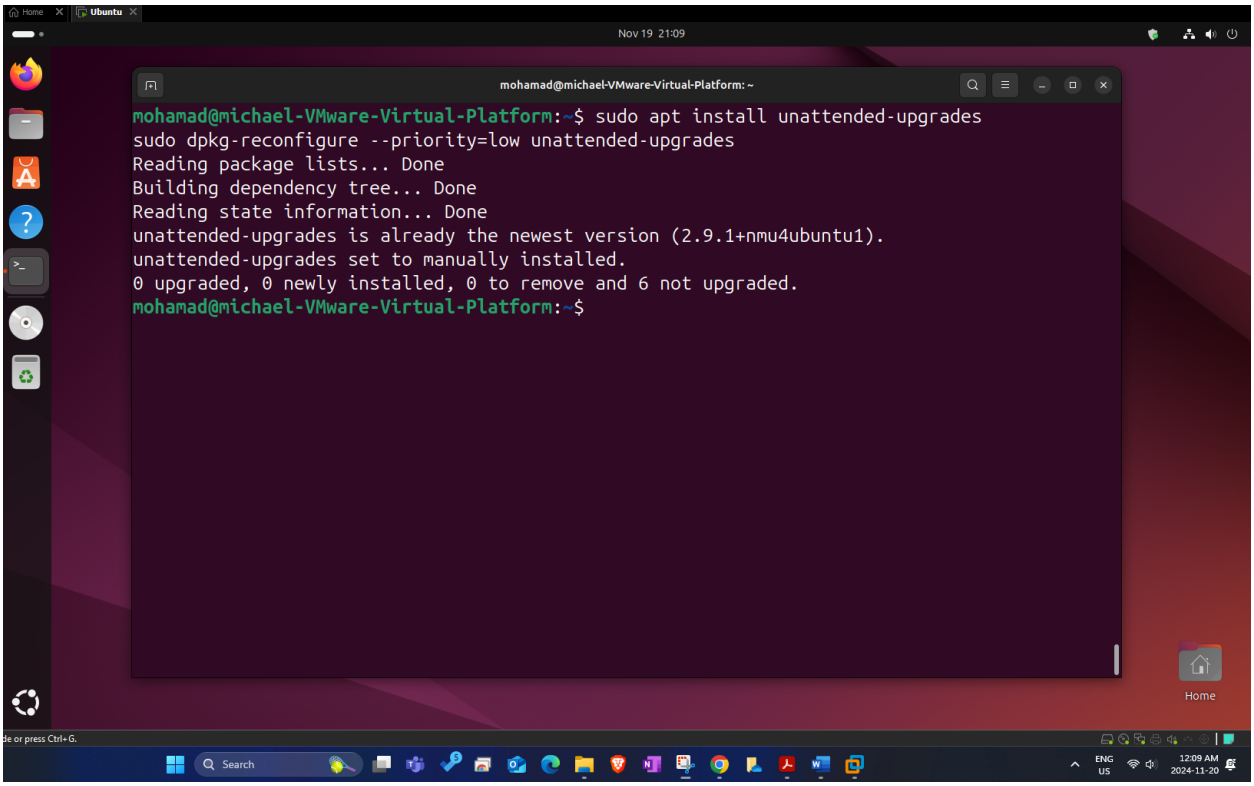
Keep software up-to-date:
Run regular updates to ensure all security patches are applied

sudo apt update && sudo apt upgrade -y



Enable unattended upgrades:

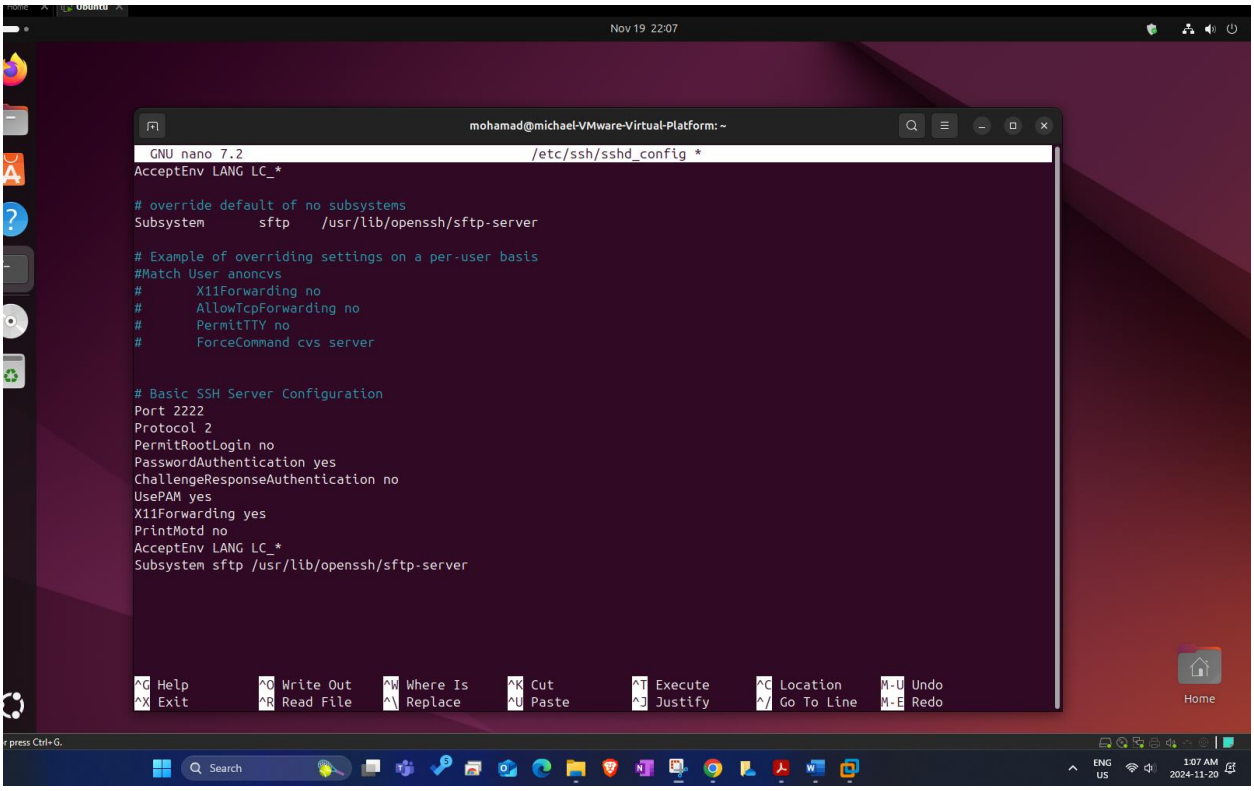
Automate updates for critical security patches:

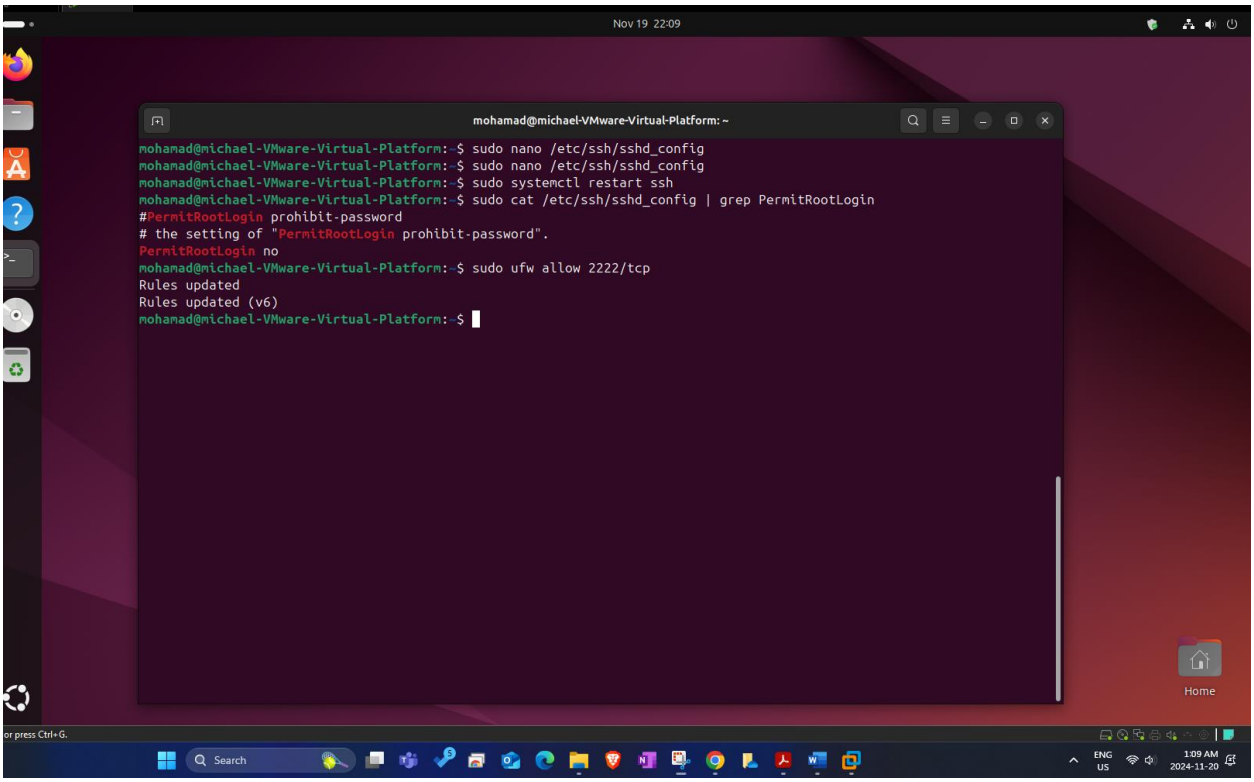


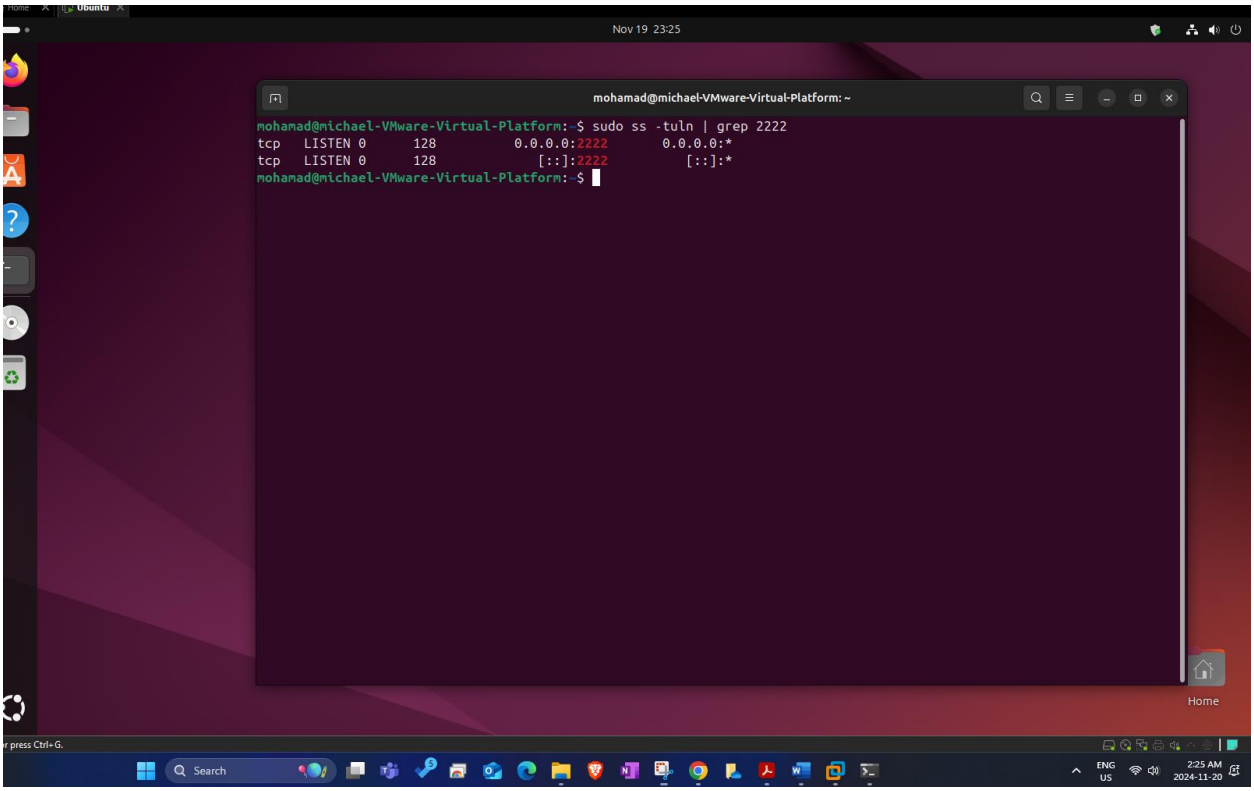
Secure SSH:

Securing SSH (Secure Shell) is a critical step to protect your system from unauthorized access and potential cyberattacks. SSH is a widely used protocol for securely accessing and managing remote systems, but its default settings can make it a target for attackers.

Disable root login:

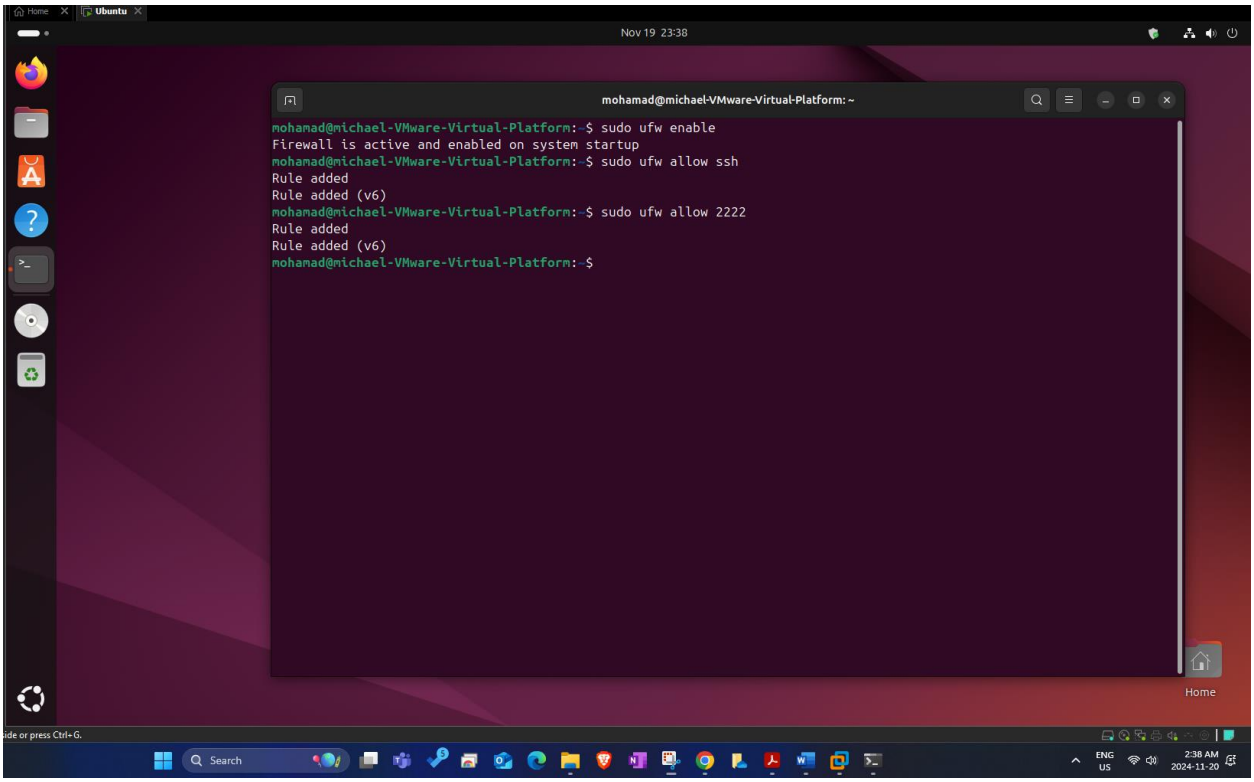

Nov 19 22:07
mohamad@michael-VMware-Virtual-Platform: ~
GNU nano 7.2 /etc/ssh/sshd_config *
AcceptEnv LANG LC_*
override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server
Example of overriding settings on a per-user basis
#Match User anoncvs
X11Forwarding no
AllowTcpForwarding no
PermitTTY no
ForceCommand cvs server
Basic SSH Server Configuration
Port 2222
Protocol 2
PermitRootLogin no
PasswordAuthentication yes
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding yes
PrintMotd no
AcceptEnv LANG LC_*
Subsystem sftp /usr/lib/openssh/sftp-server
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Home
Search
ENG US
1:07 AM 2024-11-20


Nov 19 22:09
mohamad@michael-VMware-Virtual-Platform: ~
mohamad@michael-VMware-Virtual-Platform:~$ sudo nano /etc/ssh/sshd_config
mohamad@michael-VMware-Virtual-Platform:~$ sudo nano /etc/ssh/sshd_config
mohamad@michael-VMware-Virtual-Platform:~$ sudo systemctl restart ssh
mohamad@michael-VMware-Virtual-Platform:~$ sudo cat /etc/ssh/sshd_config | grep PermitRootLogin
#PermitRootLogin prohibit-password
the setting of "PermitRootLogin prohibit-password".
PermitRootLogin no
mohamad@michael-VMware-Virtual-Platform:~$ sudo ufw allow 2222/tcp
Rules updated
Rules updated (v6)
mohamad@michael-VMware-Virtual-Platform:~$
Home
Search
ENG
US
1:09 AM
2024-11-20



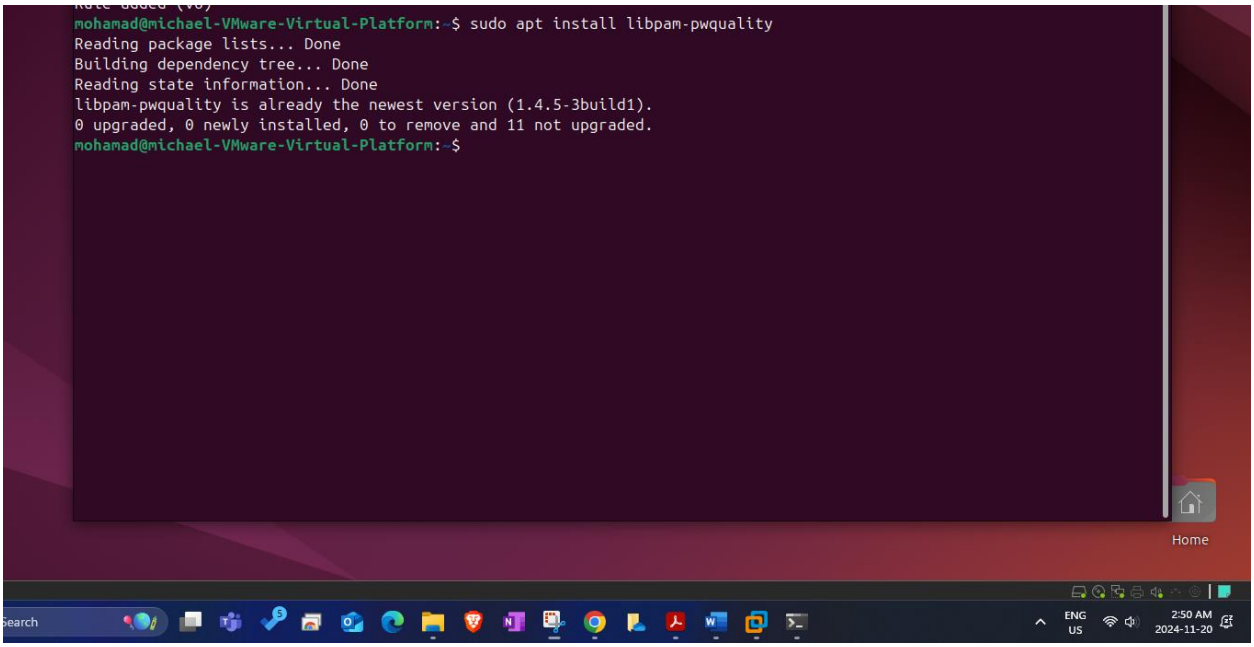
Configure a Firewall

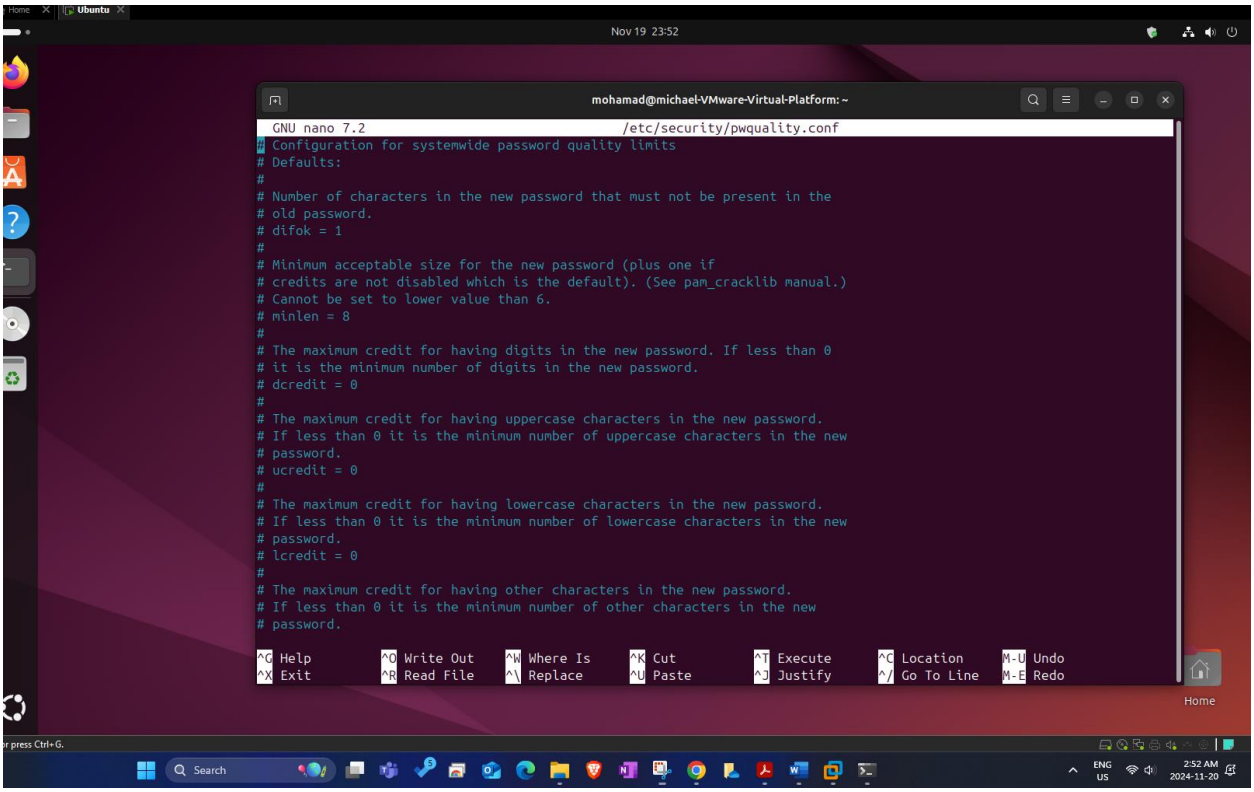
- **Benefit**: Controls which connections are allowed to the system, reducing exposure to attacks.



Use Strong Password Policies

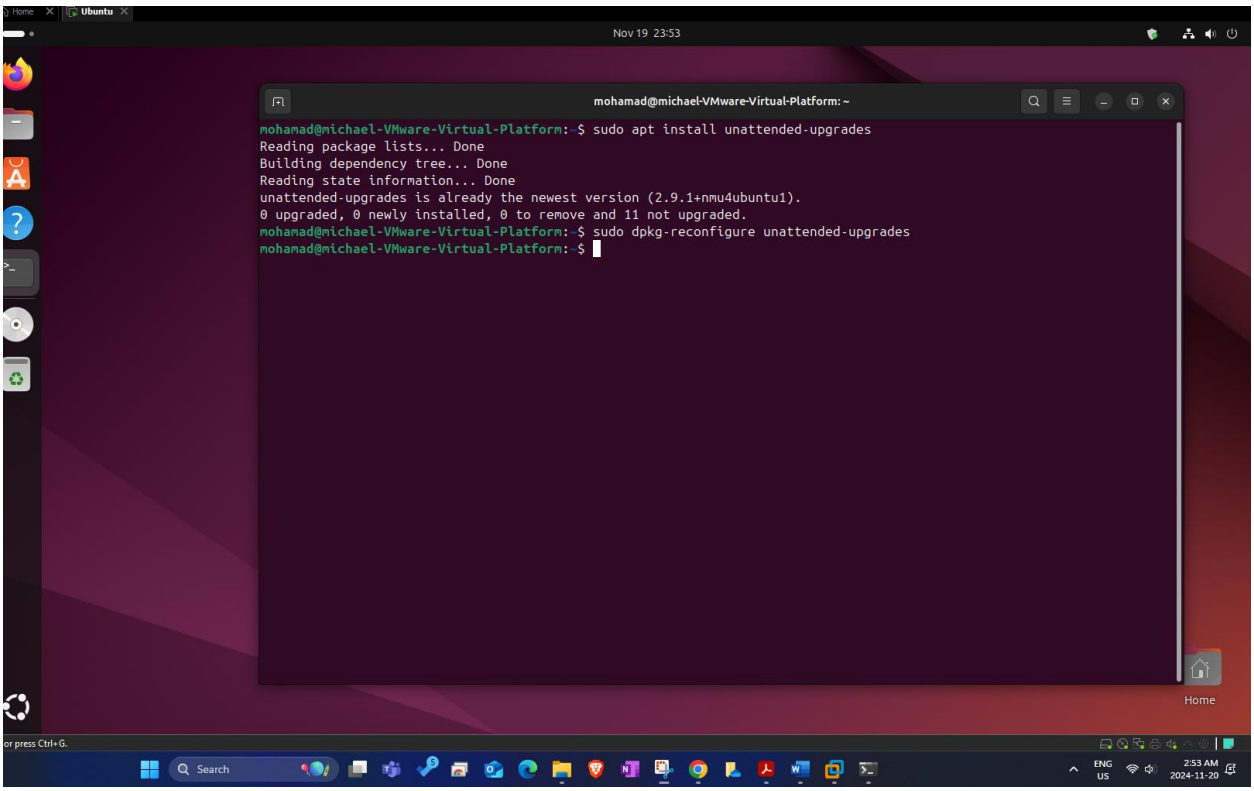
- **Benefit**: Prevents weak passwords, reducing the risk of unauthorized access.


mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libpam-pwquality is already the newest version (1.4.5-3build1).
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
mohamad@michael-VMware-Virtual-Platform:~$
Home
Search
ENG
US
2:50 AM
2024-11-20


Ubuntu
Nov 19 23:52
mohamad@michael-VMware-Virtual-Platform: ~
GNU nano 7.2 /etc/security/pwquality.conf
Configuration for systemwide password quality limits
Defaults:
#
Number of characters in the new password that must not be present in the
old password.
difok = 1
#
Minimum acceptable size for the new password (plus one if
credits are not disabled which is the default). (See pam_cracklib manual.)
Cannot be set to lower value than 6.
minlen = 8
#
The maximum credit for having digits in the new password. If less than 0
it is the minimum number of digits in the new password.
dcredit = 0
#
The maximum credit for having uppercase characters in the new password.
If less than 0 it is the minimum number of uppercase characters in the new
password.
ucredit = 0
#
The maximum credit for having lowercase characters in the new password.
If less than 0 it is the minimum number of lowercase characters in the new
password.
lcredit = 0
#
The maximum credit for having other characters in the new password.
If less than 0 it is the minimum number of other characters in the new
password.
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Home
Search
ENG
US
2:52 AM
2024-11-20

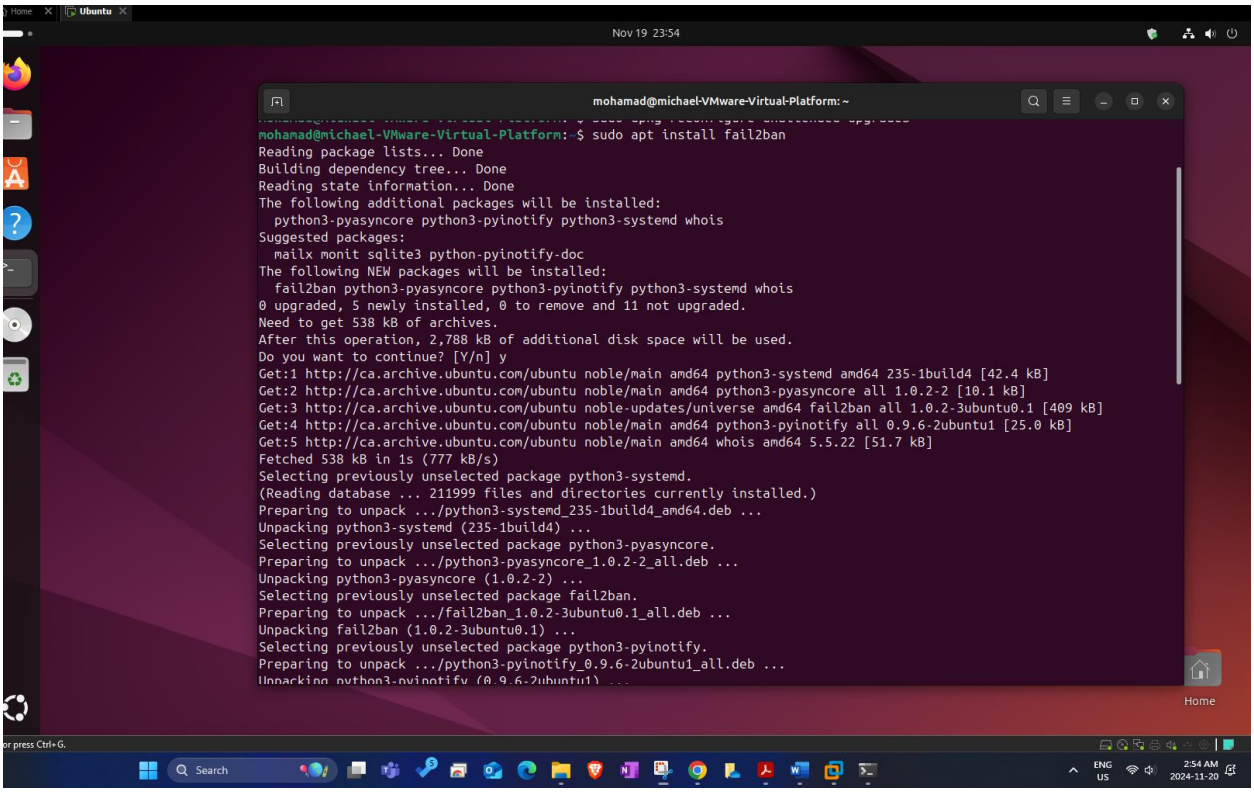
Enable Automatic Security Updates

- **Benefit**: Automatically installs critical updates to keep the system secure without manual intervention.



Use Fail2Ban for Brute-Force Protection

Benefit: Protects the system from repeated unauthorized login attempts by blocking attackers.

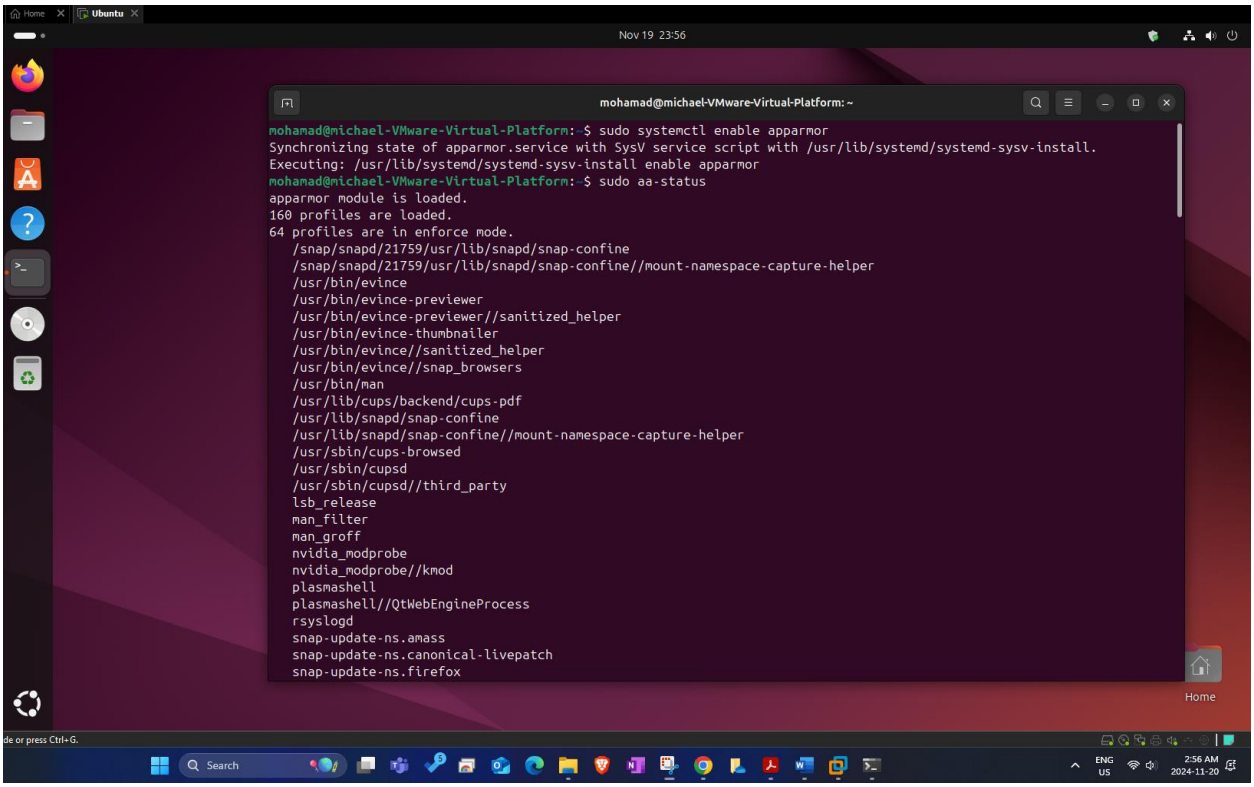


Secure Shared Files and Folders

Benefit: Protects sensitive files by restricting access to authorized users only.

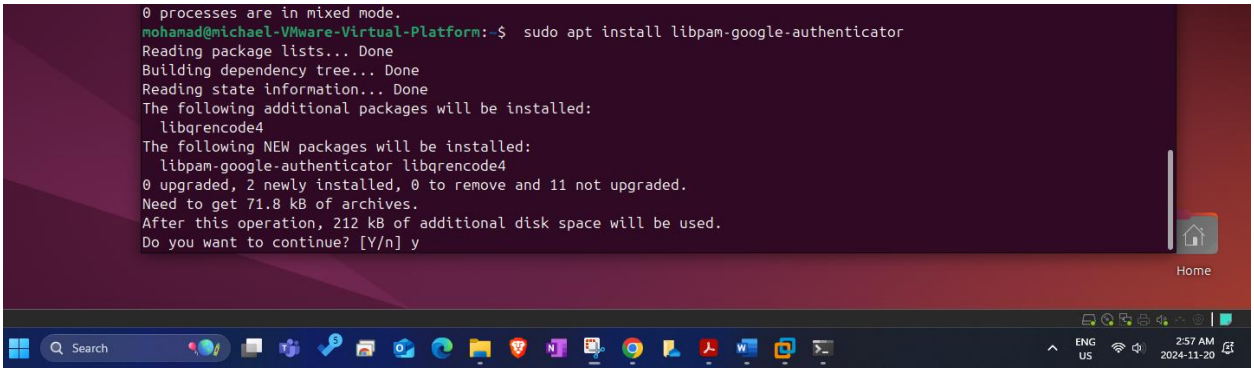
Configure AppArmor

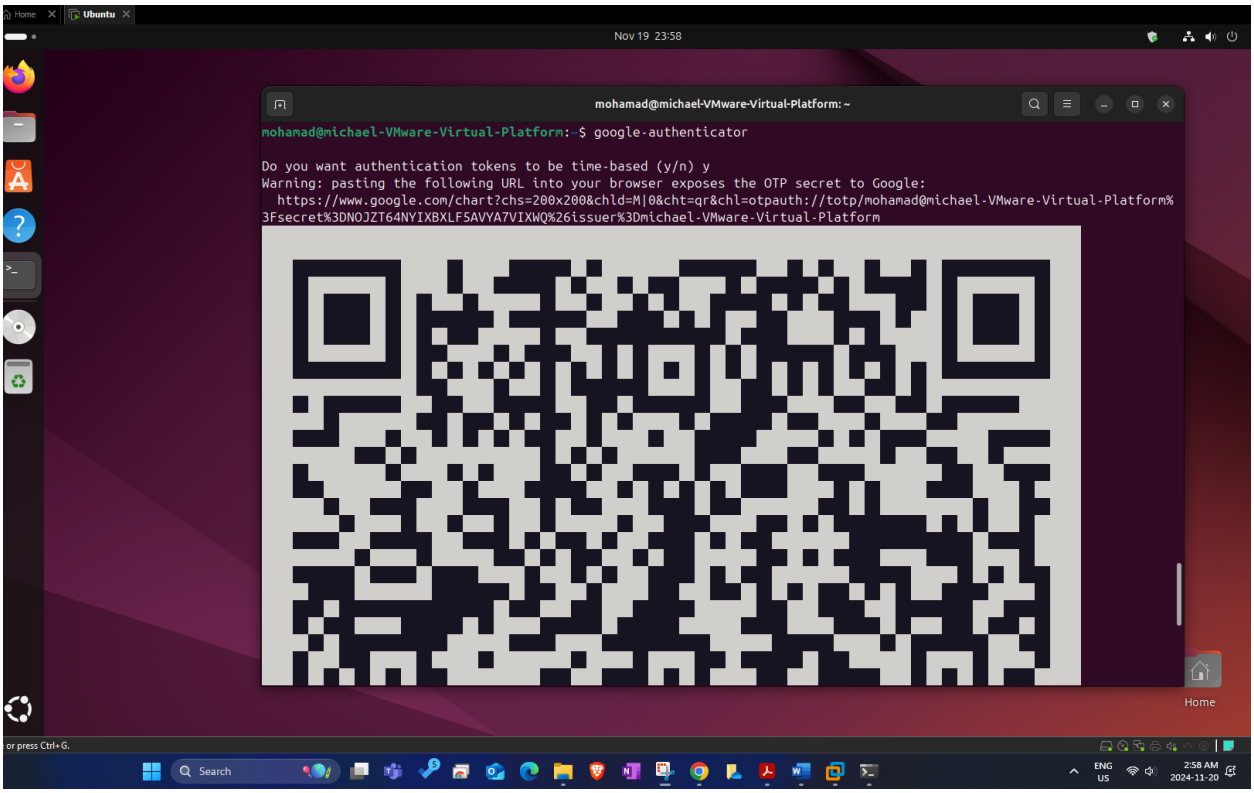
- **Benefit**: Adds extra security by limiting what applications can access on the system.



Use Multi-Factor Authentication (MFA)

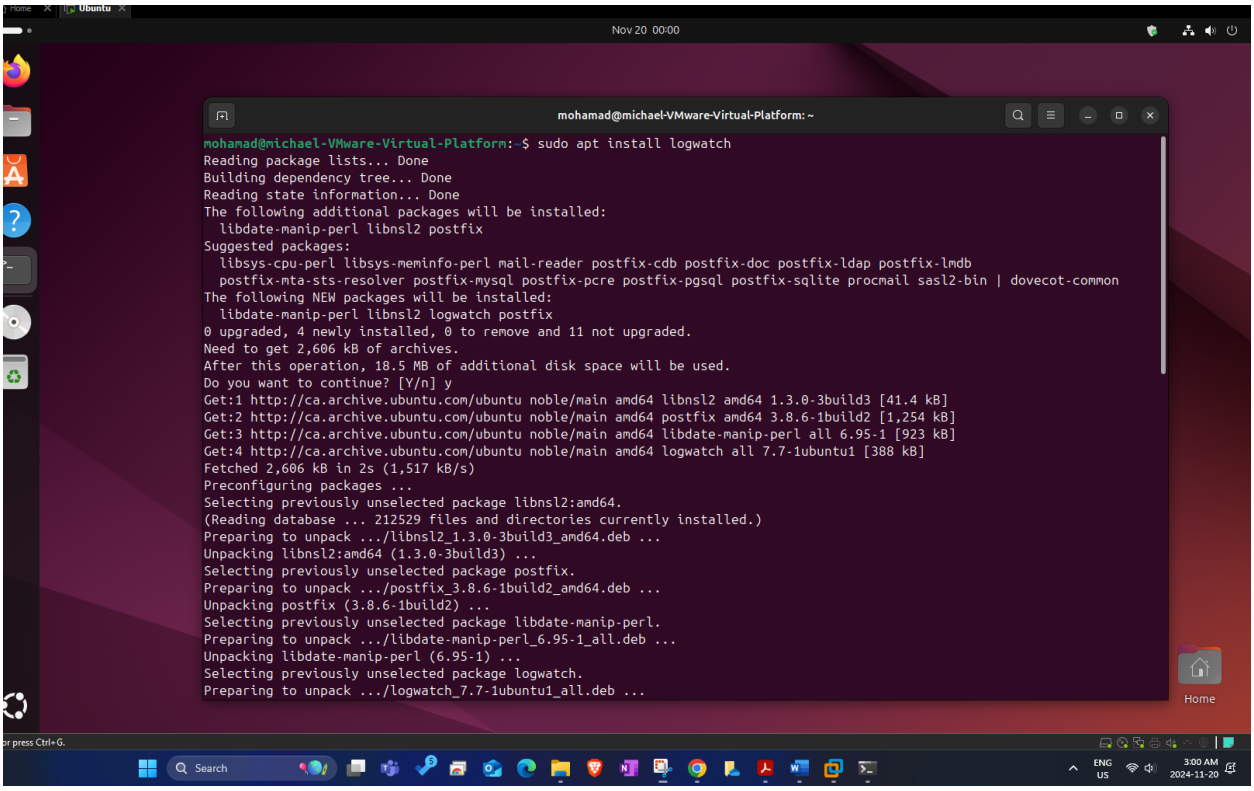
- **Benefit**: Adds an extra layer of security beyond just a password.

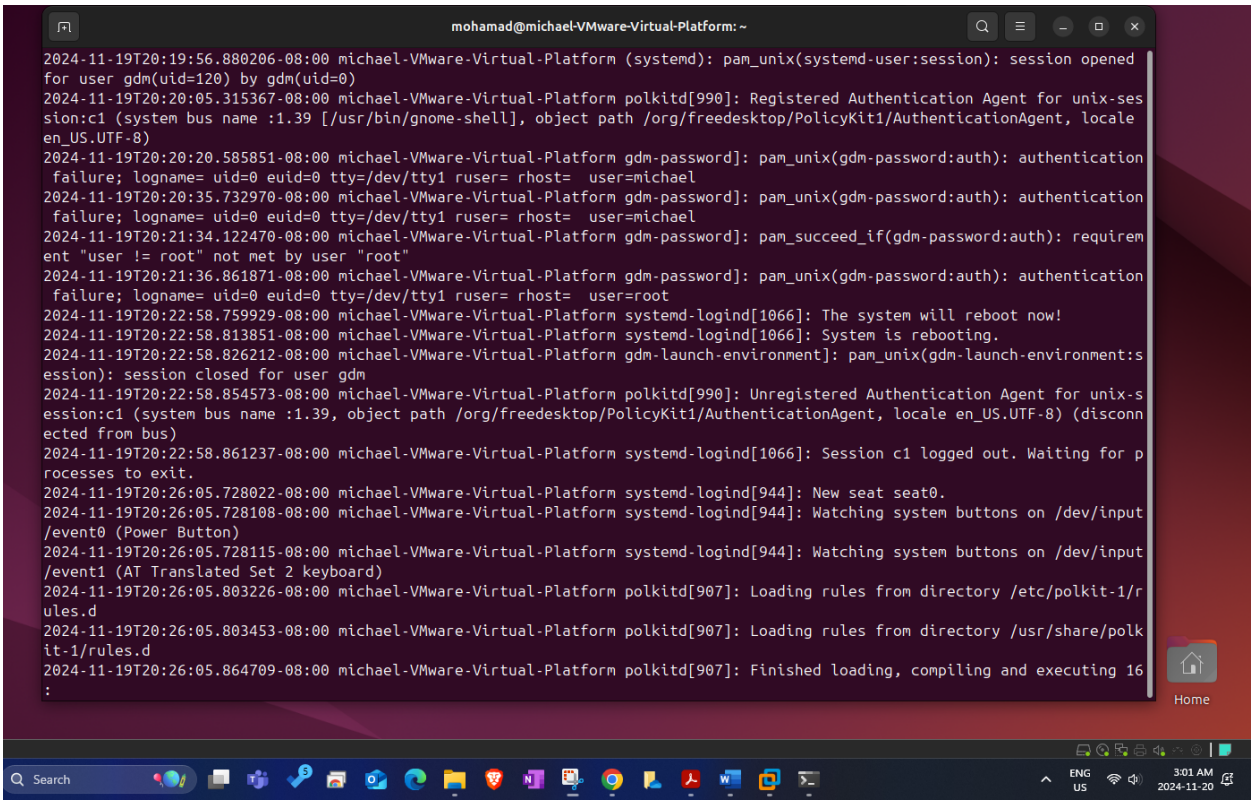




Monitor Logs

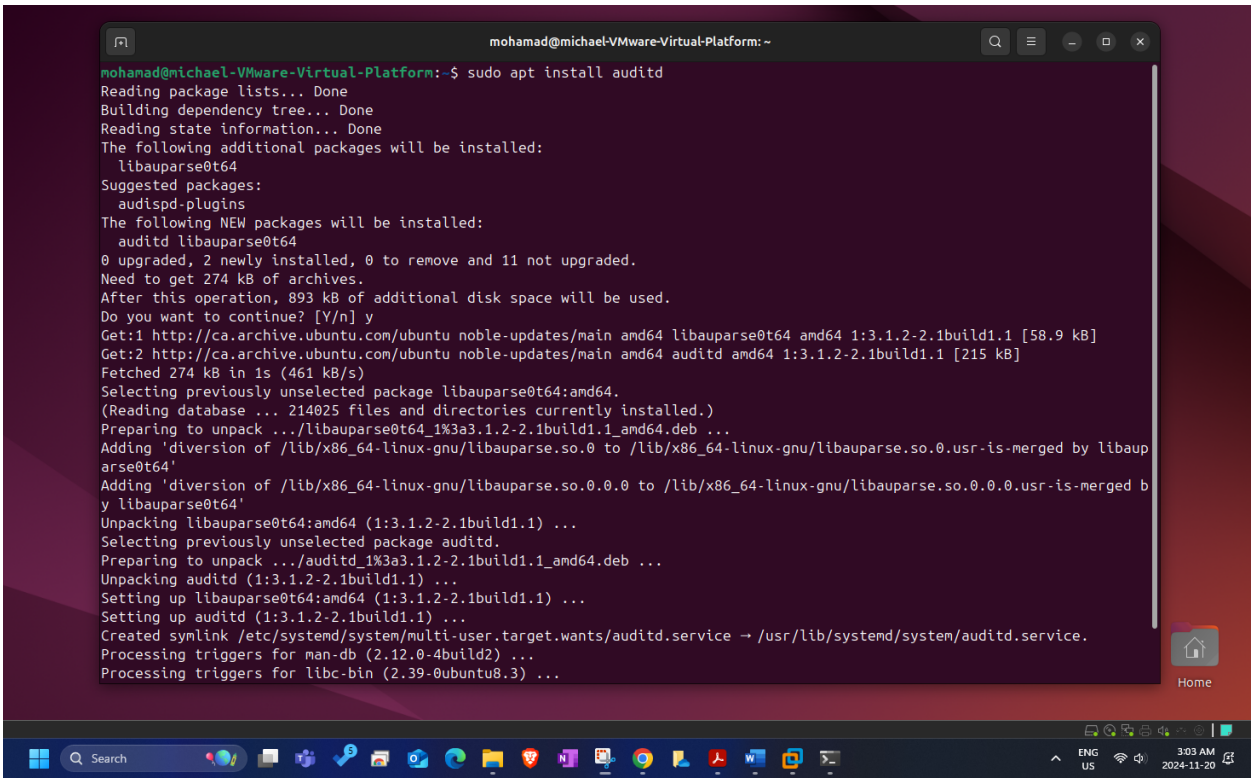
Benefit: Helps detect unusual activity by reviewing system logs.


Nov 20 00:00
mohamad@michael-VMware-Virtual-Platform: ~
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install logwatch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libdate-manip-perl libnsl2 postfix
Suggested packages:
libsys-cpu-perl libsys-meminfo-perl mail-reader postfix-cdb postfix-doc postfix-ldap postfix-lmdb
postfix-mta-sts-resolver postfix-mysql postfix-pcre postfix-pgsql postfix-sqlite procmail sasl2-bin | dovecot-common
The following NEW packages will be installed:
libdate-manip-perl libnsl2 logwatch postfix
0 upgraded, 4 newly installed, 0 to remove and 11 not upgraded.
Need to get 2,606 kB of archives.
After this operation, 18.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 libnsl2 amd64 1.3.0-3build3 [41.4 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1,254 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 libdate-manip-perl all 6.95-1 [923 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 logwatch all 7.7-1ubuntu1 [388 kB]
Fetched 2,606 kB in 2s (1,517 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libnsl2:amd64.
(Reading database ... 212529 files and directories currently installed.)
Preparing to unpack .../libnsl2_1.3.0-3build3_amd64.deb ...
Unpacking libnsl2:amd64 (1.3.0-3build3) ...
Selecting previously unselected package postfix.
Preparing to unpack .../postfix_3.8.6-1build2_amd64.deb ...
Unpacking postfix (3.8.6-1build2) ...
Selecting previously unselected package libdate-manip-perl.
Preparing to unpack .../libdate-manip-perl_6.95-1_all.deb ...
Unpacking libdate-manip-perl (6.95-1) ...
Selecting previously unselected package logwatch.
Preparing to unpack .../logwatch_7.7-1ubuntu1_all.deb ...
Home
Search
ENG
US
3:00 AM
2024-11-20



Enable Auditing

Benefit: Tracks system activities to detect suspicious behavior or unauthorized changes.


mohamad@michael-VMware-Virtual-Platform: ~
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libauparse0t64
Suggested packages:
audispd-plugins
The following NEW packages will be installed:
auditd libauparse0t64
0 upgraded, 2 newly installed, 0 to remove and 11 not upgraded.
Need to get 274 kB of archives.
After this operation, 893 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 libauparse0t64 amd64 1:3.1.2-2.1build1.1 [58.9 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 auditd amd64 1:3.1.2-2.1build1.1 [215 kB]
Fetched 274 kB in 1s (461 kB/s)
Selecting previously unselected package libauparse0t64:amd64.
(Reading database ... 214025 files and directories currently installed.)
Preparing to unpack .../libauparse0t64_1%3a3.1.2-2.1build1.1_amd64.deb ...
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0 to /lib/x86_64-linux-gnu/libauparse.so.0.usr-is-merged by libauparse0t64'
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0.0.0 to /lib/x86_64-linux-gnu/libauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:amd64 (1:3.1.2-2.1build1.1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a3.1.2-2.1build1.1_amd64.deb ...
Unpacking auditd (1:3.1.2-2.1build1.1) ...
Setting up libauparse0t64:amd64 (1:3.1.2-2.1build1.1) ...
Setting up auditd (1:3.1.2-2.1build1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /usr/lib/systemd/system/auditd.service.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
Home
Search
ENG
US
3:03 AM
2024-11-20